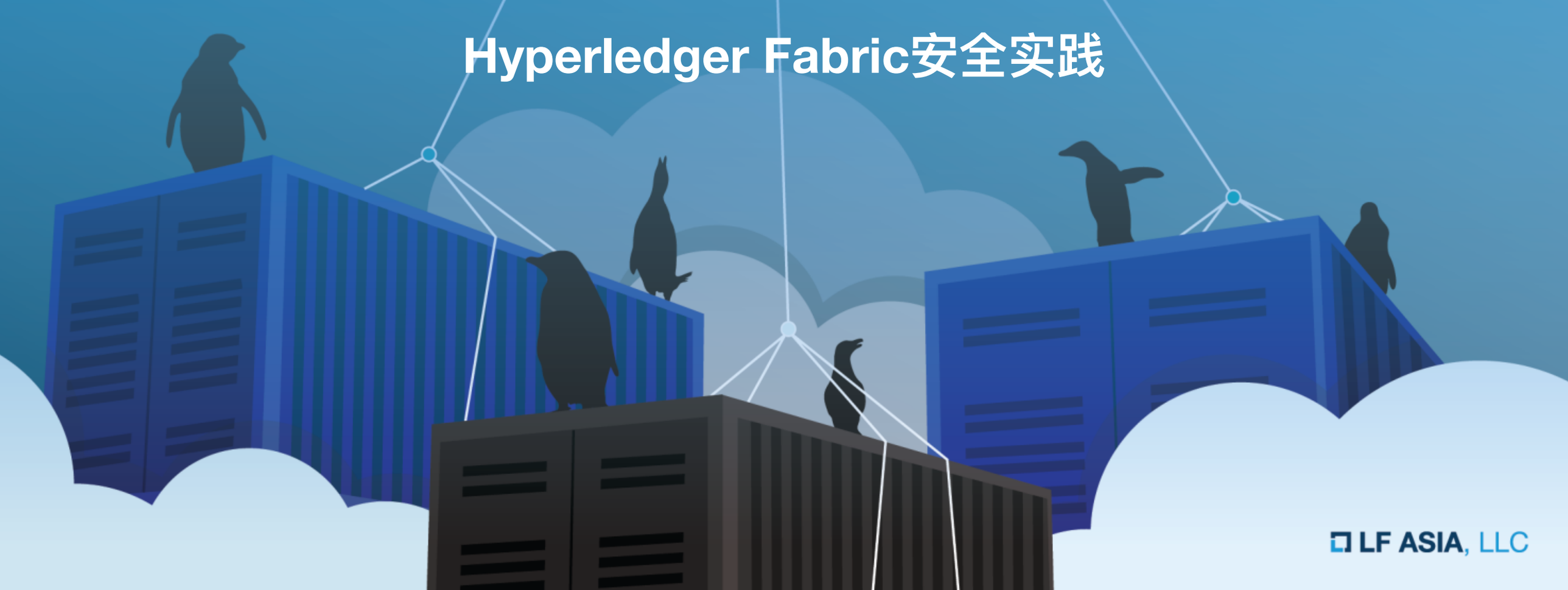
LINUXCON containercon CHINA 中国 CLOUDOPEN

THINK OPEN

开放性思维

点融区块链云服务

Hyperledger Fabric安全实践



LF ASIA, LLC

自我介绍 - 史锋锋

点融 / 资深架构师

区块链云服务平台

EMC / 资深架构师

Avamar Data Protection

爱立信（中国）通信有限公司 / 高级软件工程师

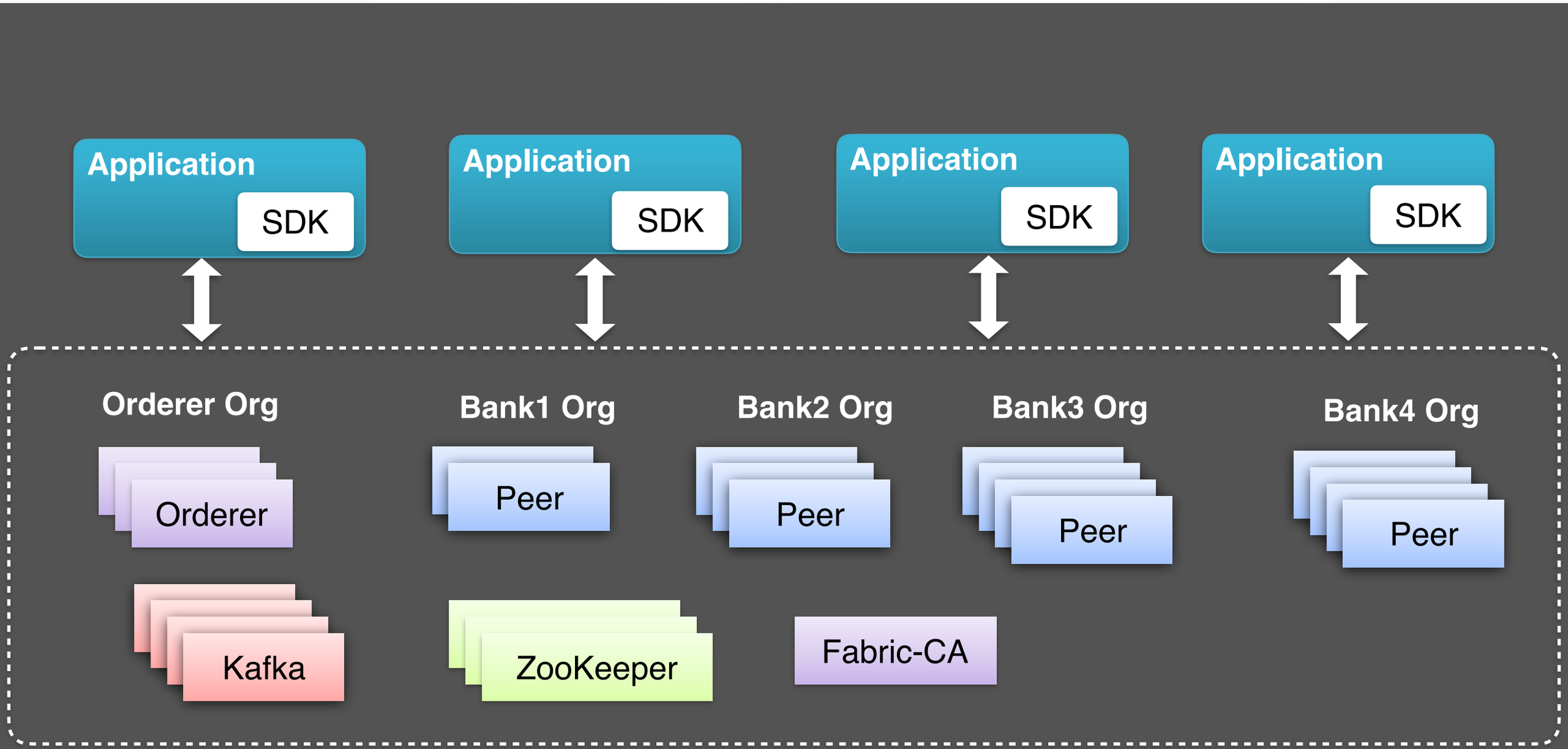
流媒体移动电视、LTE Broadcast

目前专注于企业级区块链技术的研究

提纲

- Hyperledger Fabric简介
- 区块链应用落地的安全挑战
- 点融区块链云服务的安全实践

Hyperledger Fabric简介

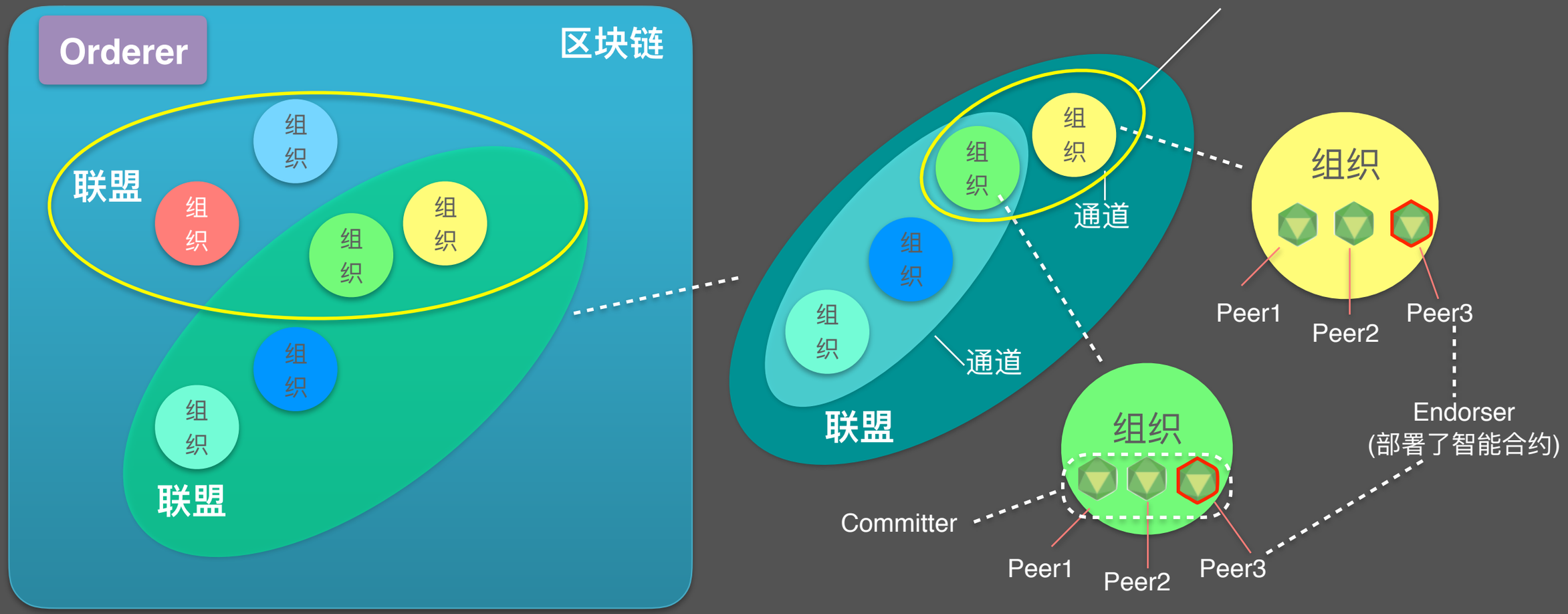


Fabric 区块链是一个授权网络

Hyperledger Fabric简介

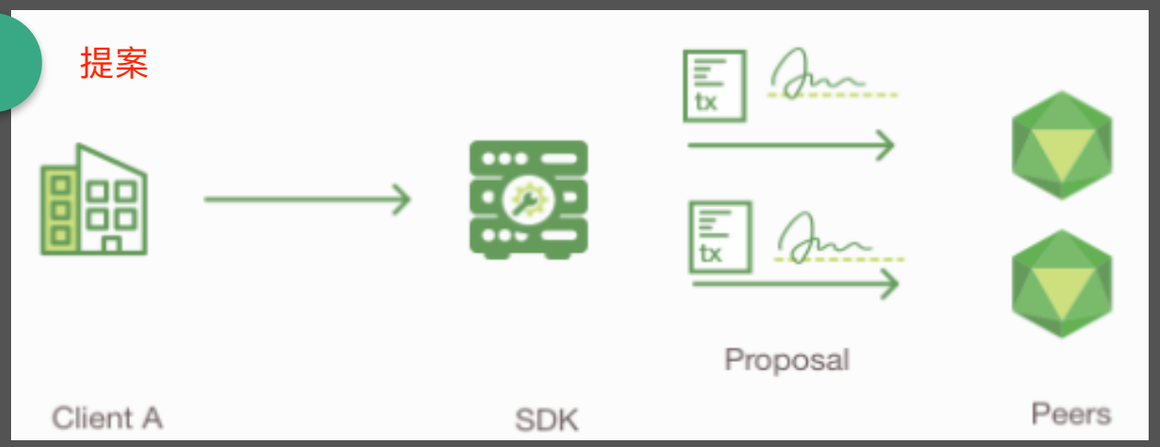
Fabric 区块链本质上是一个分布式的共享账本

每个“通道”都有一个独立的账本，
仅在加入通道的组织之间共享



Hyperledger Fabric简介

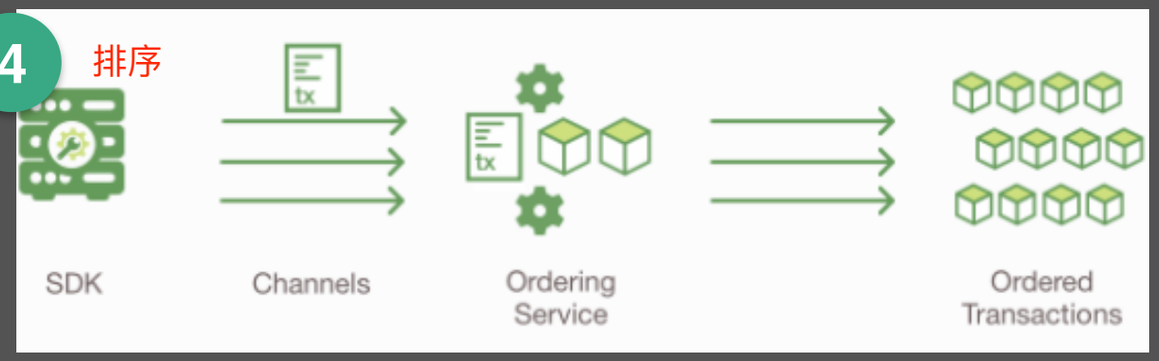
1 提案



2 背书

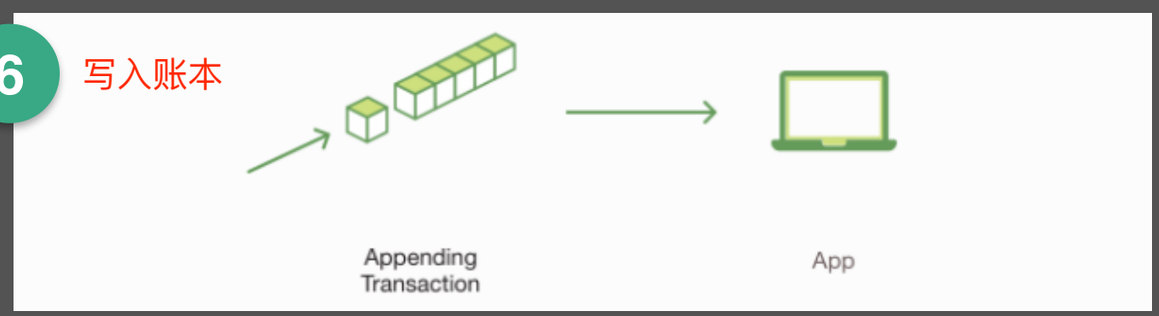
3 验证

4 排序



5 交易验证

6 写入账本



Hyperledger Fabric安全特性

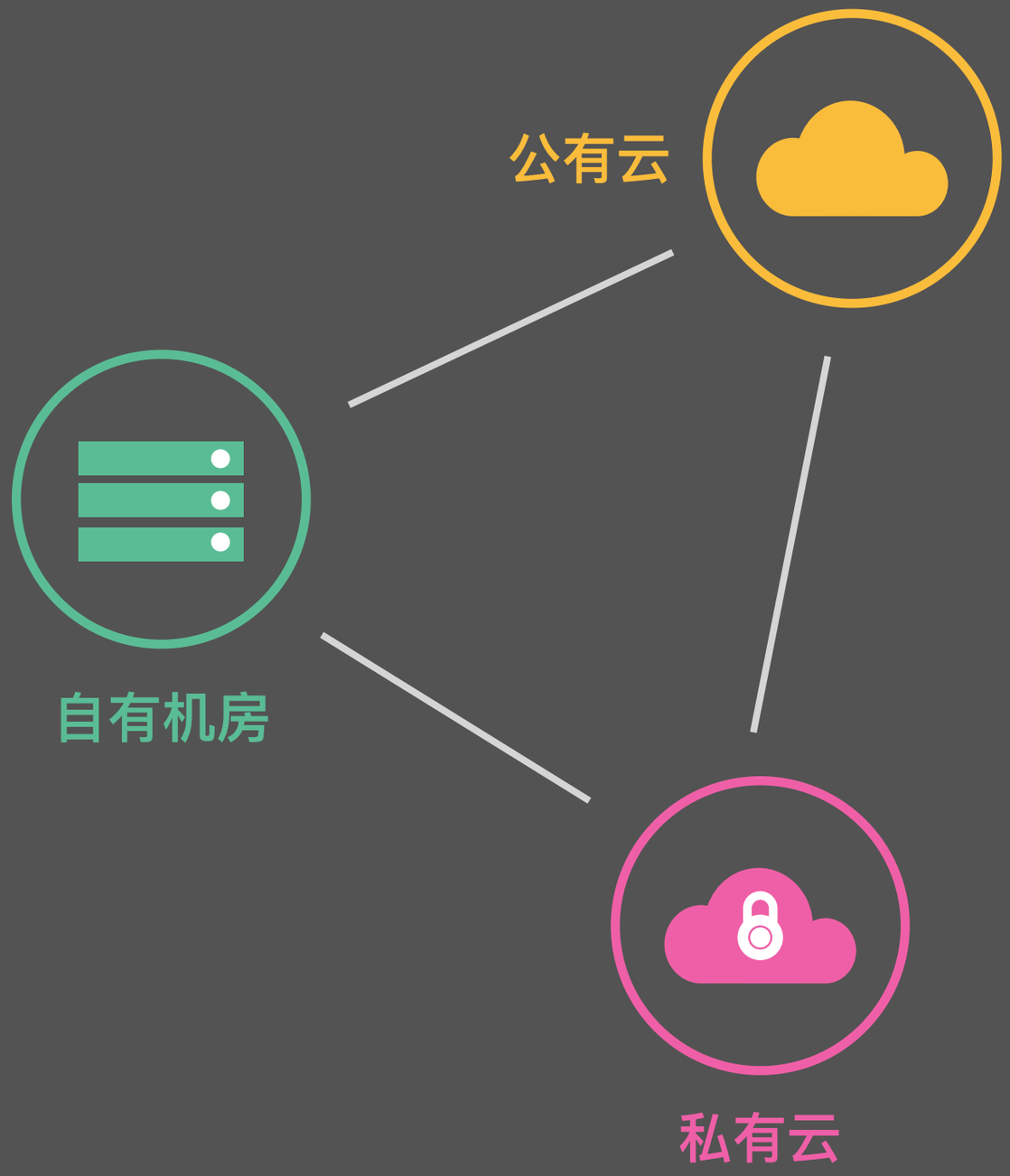
- 强大的身份认证
- 灵活的策略管理
- 智能合约的访问控制
- 账本数据加密

区块链应用落地的安全挑战

- 如何在区块链参与方异构的网络环境中组建联盟链?
- 如何简单有效的控制区块链参与方的权限?
- 如何高效的实施与业务相匹配的安全要求?

安全挑战1 - 异构网络环境组建联盟链

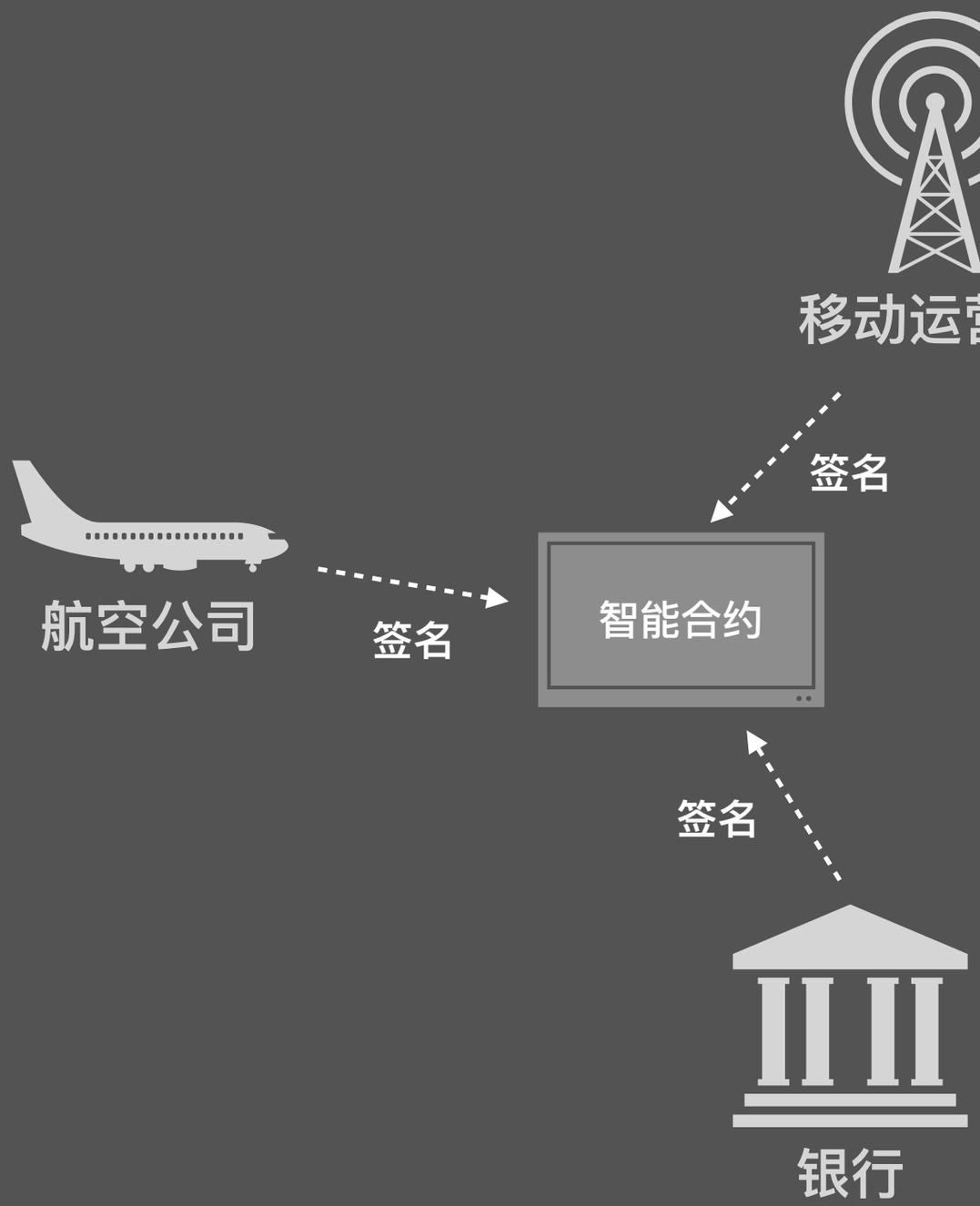
- 组建联盟链网络
- 复杂网络环境的隔离
- 区块链节点的安全加固



安全挑战2 - 区块链参与方的权限控制

数字积分的联盟链 - 智能合约签名

- 参与方背书智能合约
- 安装智能合约
- 初始化智能合约 - 背书策略
- 智能合约调用
- 智能合约升级



安全挑战2 - 区块链参与方的权限控制

背书合约
审核合约
安装合约
实例化到通道
复用合约
升级合约

区块链应用

智能合约

新组织加入联盟
新组织加入通道
新节点加入通道
背书策略更新

Fabric 区块链的领域模型：
联盟、组织(MSP)、通道、策略

新节点加入
资源扩容

Fabric 区块链物理网络

安全挑战3 - 业务相匹配的密钥安全要求

软件实现

USB KEY

硬件加密机

让用户只需关注于业务实现，平台负责构建安全的区块链网络

点融区块链云服务

提供企业级的区块链基础设施服务

帮助用户轻松创建、管理和维护区块链

快速开发、部署区块链应用

分分钟创建区块链

跨云部署

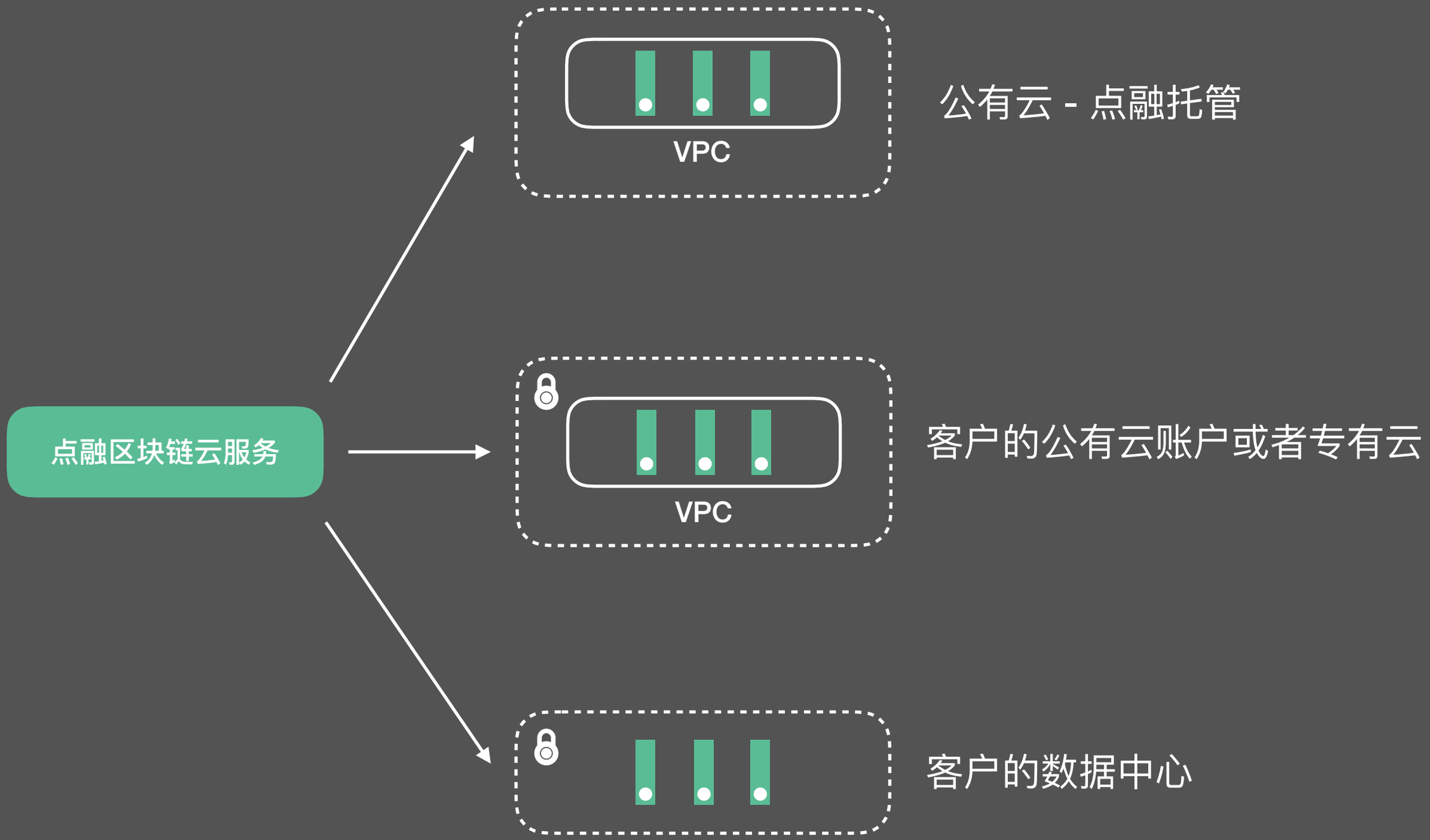
随需弹性扩展

可视化管理“链”

线上申请/线下审批

管理智能合约

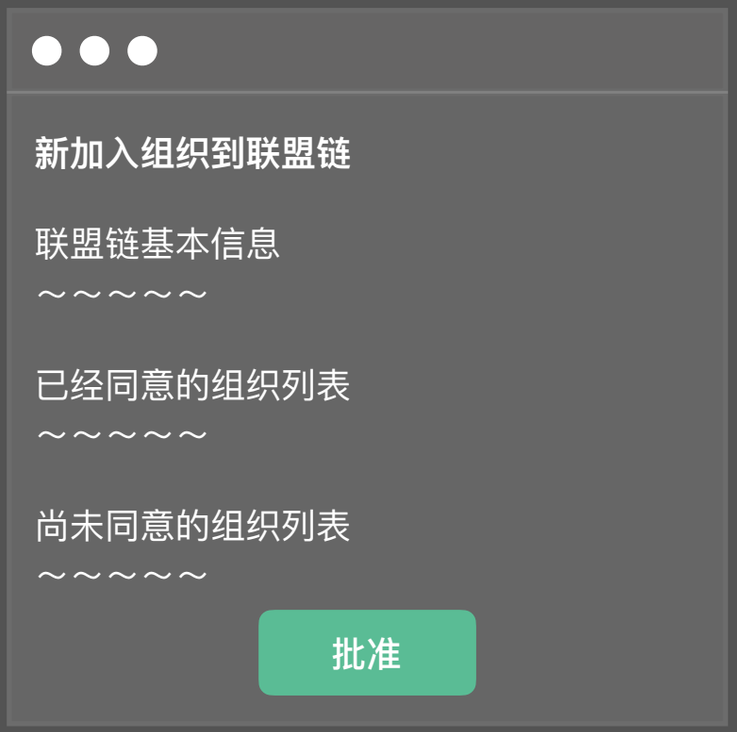
更开放的联盟链



更可控的权限管理

不同组织共同组建一个联盟链

更可控的权限管理



点融区块链云服务不保存用户的任何私钥

更可控的权限管理

数字积分的联盟链

同意新成员（零售公司）加入通道的共识过程

航空公司

零售公司申请加入到通道

数字积分联盟链

银行	已同意
移动运营商	未同意

同意加入

移动公司

零售公司申请加入到通道

数字积分联盟链

银行	已同意
航空公司	未同意

同意加入

银行

零售公司申请加入到通道

数字积分联盟链

航空公司	未同意
移动公司	未同意

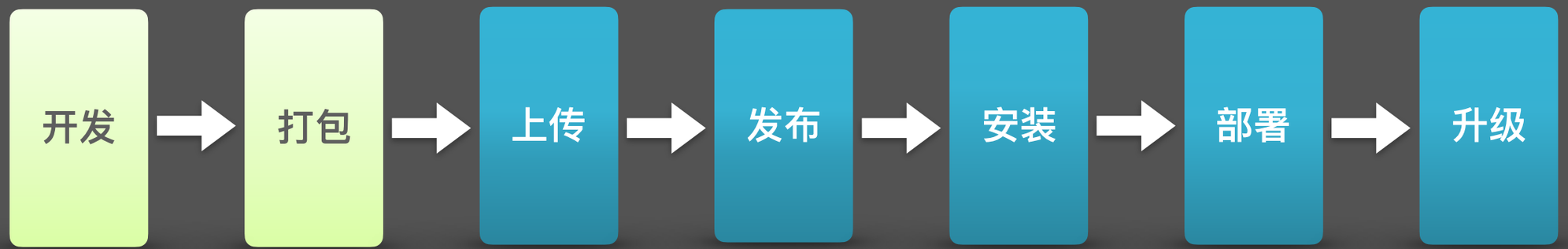
已同意

更可控的权限管理

提供“智能合约打包工具”打包智能合约
- 导出代码，以供审核
- 支持NodeJS，Golang语言

发布到不同的区块链，
合约得以复用

在线实例化
可视化的方式指定背书策略



通过点融区块链客户端
安全上传智能合约

在线安装
多节点批量安装

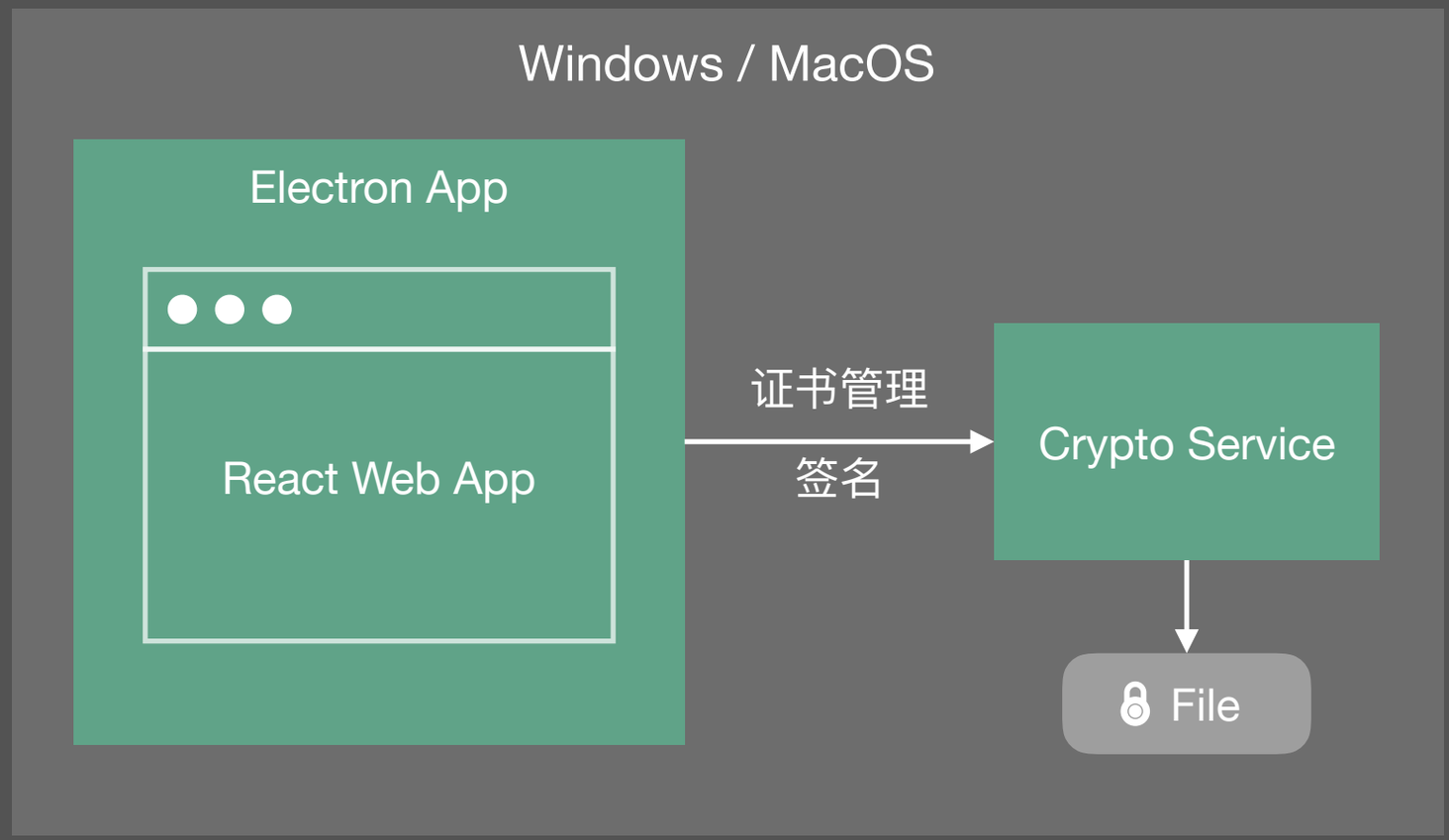
多节点同时升级

更可控的权限管理

操作分类	具体操作	发起人	审批人	是否要收集多方签名
联盟管理				
	新建联盟	盟主区块链管理员	盟主区块链管理员	否
	新组织加入联盟	盟主区块链管理员	盟主区块链管理员	否
通道管理				
	新建通道	盟主区块链管理员	盟主区块链管理员 加入该通道的成员组织管理员	是（目前支持ANY策略）
	往通道加组织	盟主区块链管理员	盟主区块链管理员 加入该通道的成员组织管理员	是（目前支持MAJORITY策略）
	往通道加节点	peer节点所属组织的管理员	peer节点所属组织的管理员	否
智能合约管理				
	上传智能合约	任意组织管理员	任意组织管理员	否
	发布智能合约	任意组织管理员	任意组织管理员 该链上的其他组织管理员	是（目前支持ANY策略）
	安装智能合约	peer节点所属组织的管理员	peer节点所属组织的管理员	否
	初始化智能合约	发布合约的组织管理员	发布合约的组织管理员	否
	升级智能合约	初始化智能合约的管理员	初始化智能合约的管理员	否

更包容的加密方案

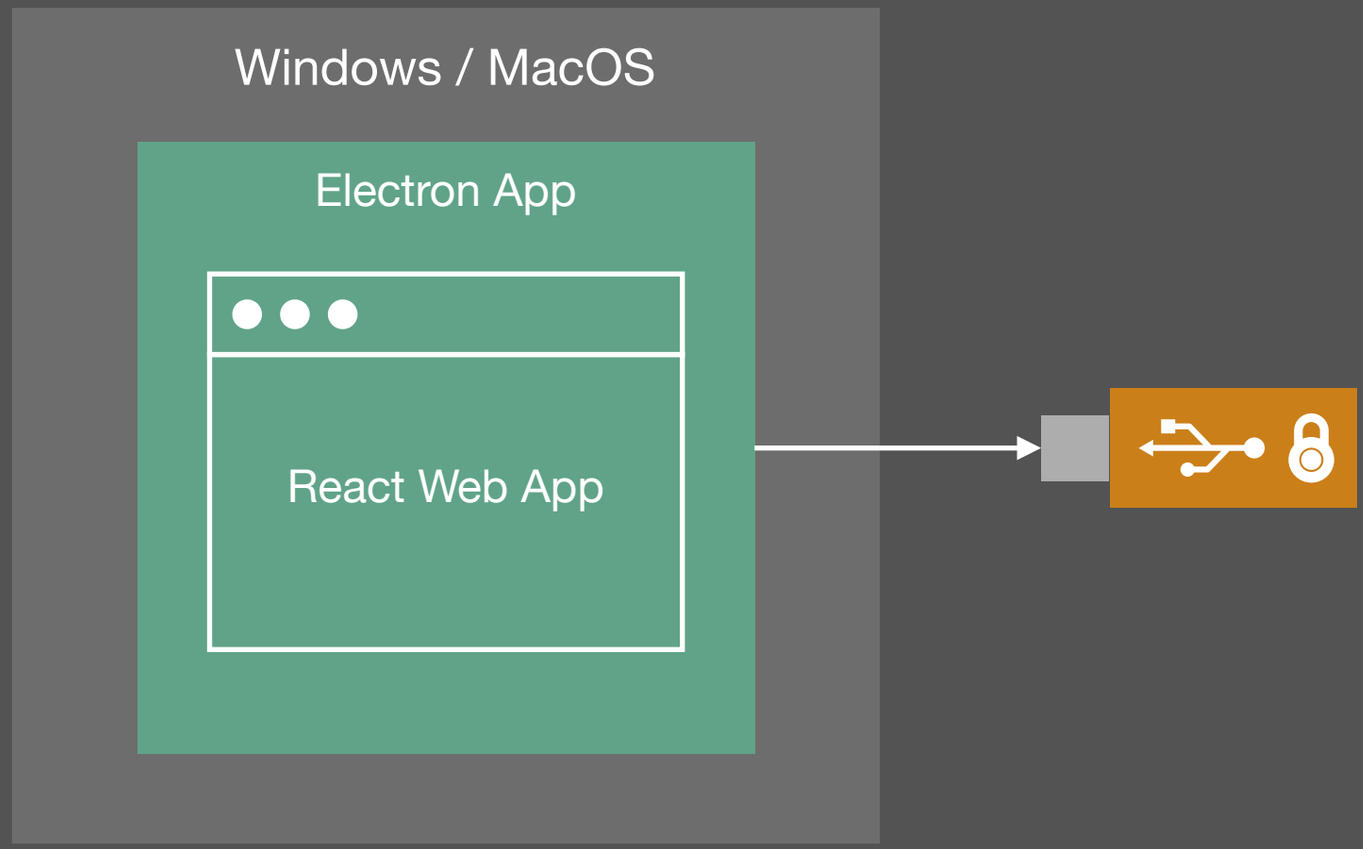
加密文件的存储证书



点融区块链客户端

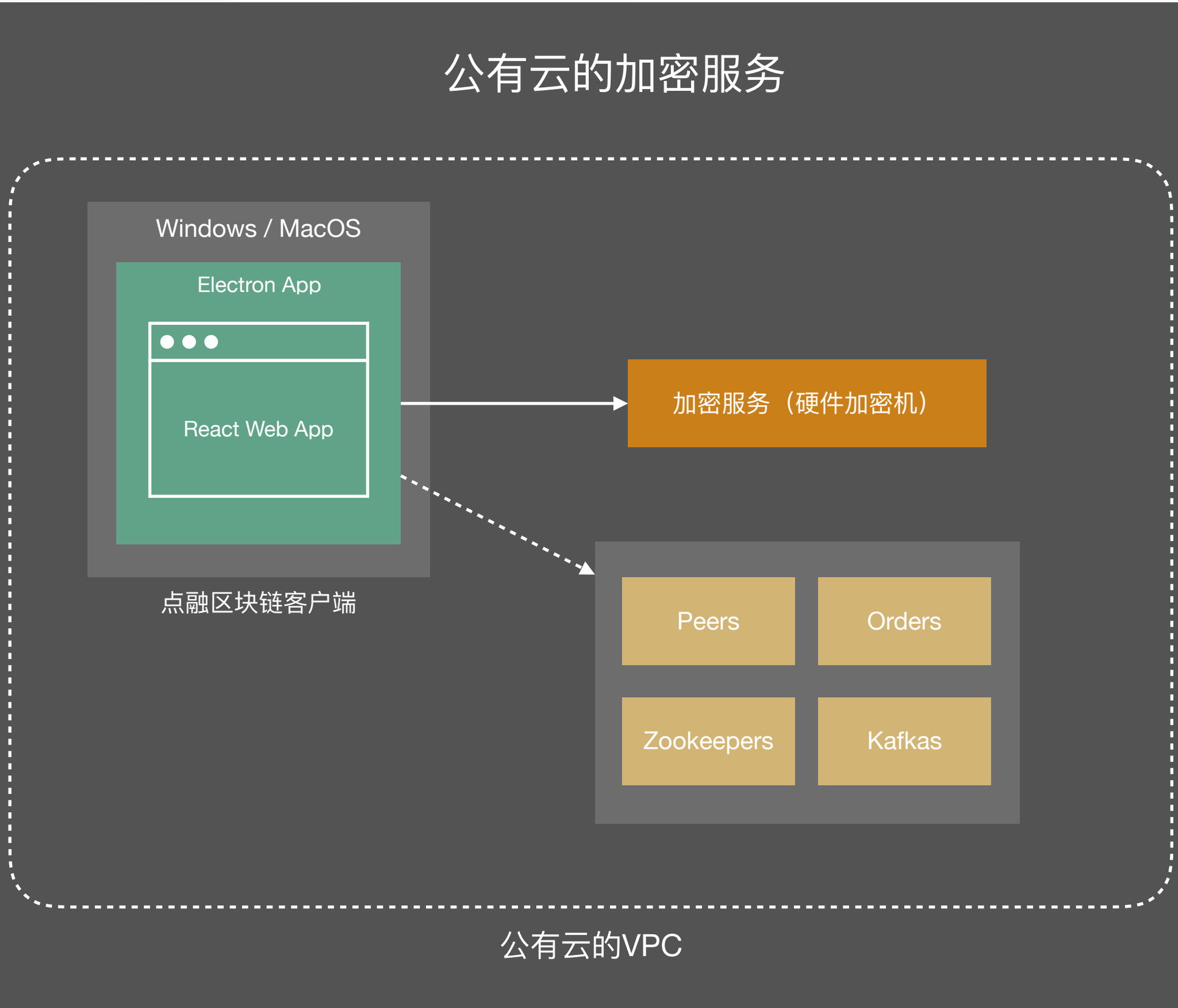
更包容的加密方案

外接的加密硬件

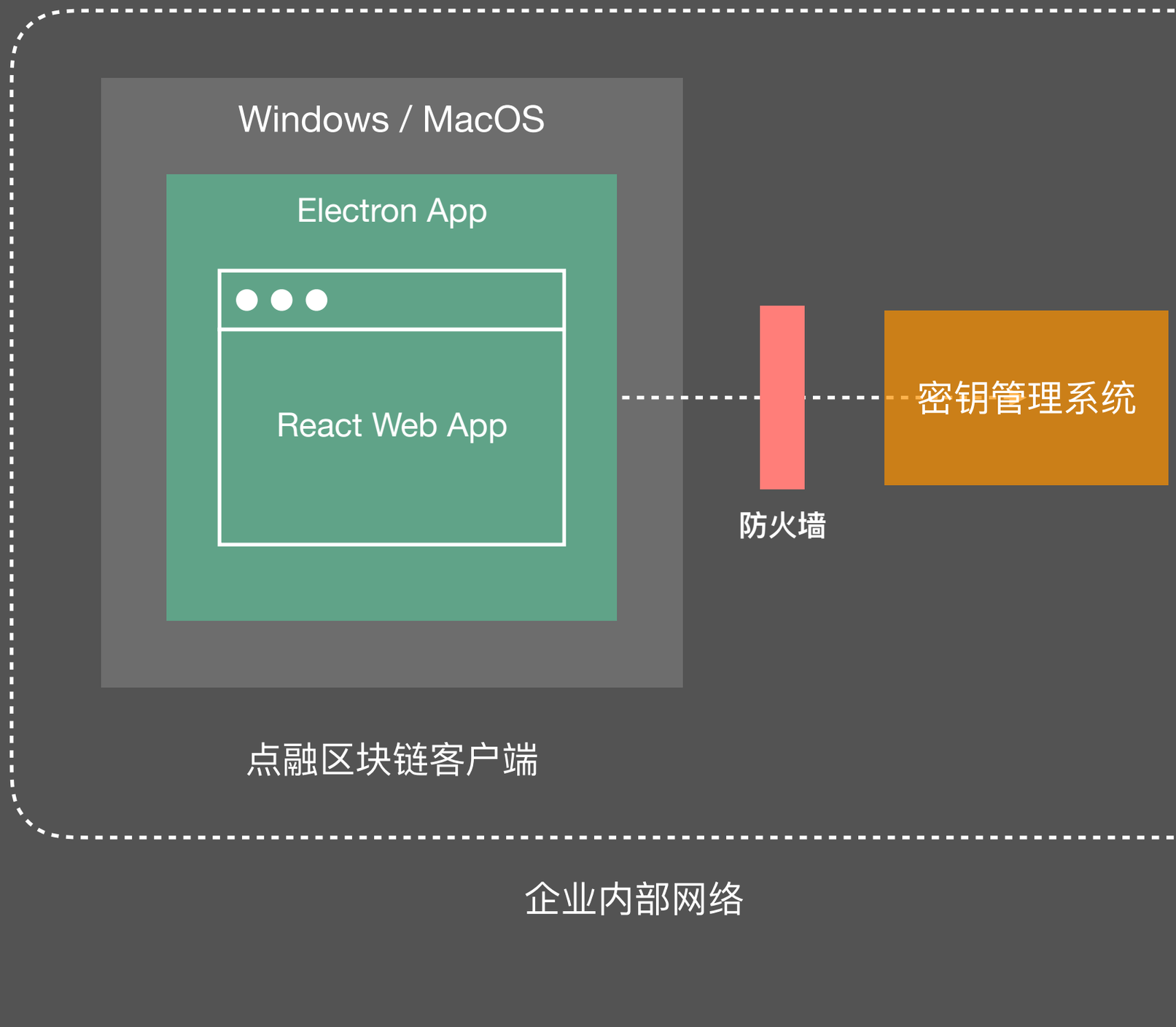


点融区块链客户端

更包容的加密方案


公有云的加密服务
Windows / MacOS
Electron App
React Web App
点融区块链客户端
加密服务（硬件加密机）
Peers
Orders
Zookeepers
Kafkas
公有云的VPC

更包容的加密方案


对接企业内部密钥管理系统
Windows / MacOS
Electron App
React Web App
密钥管理系统
防火墙
点融区块链客户端
企业内部网络

点融区块链云服务

区块链应用市场

智能合约市场

区块链底层平台
(Fabric、Corda)

公有云、外部节点、混合云
(阿里云、UCloud、OpenStack ...)

点融区块链云服务

应用开发 SDK

智能合约打包工具

点融区块链
客户端

配套工具

总结

- 更开放，更安全的联盟链
- 更可控，更方便的权限控制
- 更包容，更灵活的加密方案

欢迎大家免费体验

https://baas.dianrong.com

谢谢

点融区块链云服务交流群

邮箱: baas-support@dianrong.com